UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/415,293	10/08/1999	EARL T. CARTER	062891.0324	4623

7590 04/23/2004

SCOTT T MORRIS
BAKER & BOTTS LLP
2001 ROSS AVENUE
DALLAS, TX 752012980

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2132	14

DATE MAILED: 04/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/415,293	CARTER, EARL T.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17 and 19-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17 and 19-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This communication is in response to applicants' amendment received on April 05, 2004. Claims 1, 7, 11, 13, 14 and 20 are amended, claim 21 is newly added and claim 18 is cancelled.

It is acknowledged that the amendments of the claims and the addition of the new claim do not introduce any new matter to the claimed invention.

Applicants' arguments have been fully considered but they are not persuasive.

Applicants' arguments are all in relation to the new limitations added to claims 1, 7, 13, 14 and 20. The applicants' arguments are responded in the context of rejecting these claims as follows.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-5, 7-17 and 20-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Hile et al. (5,319,776) (hereinafter Hile).

With respect to claims 1, 7, 14 and 20, Hile discloses:

"Maintaining a state table". See, for example, column 2, lines 36-42.

"The state table indexed such that inputs comprising a current state and a current character yield an output of a new state, the new state related to an indication of an attack on a computer network". See, for example, column 4, line 59-column 5, line 21 where the machine state at start is zero and every next state and every incoming character are corresponding to the recited current state and current character, respectively, which are applied (inputted) to the state table to determine the next state of the machine. At the end, if checking of all characters of a string results in a predetermined machine state a virus match (intrusion detection) has occurred (indication of an attack).

"A state machine communicatively coupled to the state table." See, for example, Fig. 1 where the state machine 32 is coupled to the state table 34.

"Maintaining the current state". See, for example, Figure 3, where after each comparison step the resulting new state is maintained to be used as a current step for the next comparison step.

"Receiving, at a state machine of an intrusion detection device, an input stream destined for a first network device to be protected by the intrusion detection device, the input stream received at the state machine prior to reaching the first network device and

comprising a plurality of characters, wherein the first network device is operable to execute a program."

Hile discloses a virus detection technique for inspecting a data stream that either being transmitted between two computers communicating over network architecture or being copied from a removable medium onto a storage medium of a computer system (see, for example, abstract; column 1, lines 19-32; column 2, lines 4-11). Hile further discloses a state machine that receives the data stream coming from a source computer before reaching a destination computer (see, for example, Fig. 1 and column 3, lines 7-30; column 4, lines 47-58). The incoming data stream is checked character by character in the state machine before reaching the destination (see column 4, lines 7- 26). Hile also discloses that his invention protect a computer system before the virus spreads in the computer system (see, for example, column 2, lines 4-11). Moreover, Hile discloses that his invention is capable of being implemented in software or hardware (see, for example, column 3, lines 56-61) and some or all of the modules (i.e., such as the state machine, state table, buffer and alert user mechanism) could be implemented in hardware, as in the form of add on circuitry (column 10, lines 23-27). Thus, the state machine could be implemented in a separate device as an intrusion detection device rather than in the protected destination computer (corresponding to the recited first network device), for example, in conjunction with a firewall of a network.

"Selecting a first character of the input stream as the current character; and comparing the current character and the current state to the state table to generate a new state". See, for example, column 4, line 66-column 5, line 20. The process of

searching through a string of characters as disclosed by Hile for determining whether a virus signature exist in the input stream (see column 4, line 59-column 5, line 21) is very similar to the claimed invention and discards the first character before selecting a next character of the input stream.

"Transmitting the copy of the input stream to the first network device if an attack on the computer network is not detected." Hile discloses that the input stream is transmitted to the destination medium if no virus signature detected in the stream (column 2, lines 12-35).

Referring to claims 2 and 15, Hile discloses:

"Initializing the current state to an initial state". See, for example, column 4, lines 64-66.

Referring to claims 3, 11 and 16, Hile discloses:

"Setting the current state equal to the new state; selecting a next character as the current character, the next character appearing subsequent to the first character in the input stream; and repeating the comparing step". See, for example, column 4, line 59-column 5, line 21.

Referring to claims 4, 12 and 17, Hile discloses:

"Recognizing the new state as indicative of an attack upon the computer network". See, for example, column 5, lines 17-21.

Referring to claim 5, Hile discloses:

"Sounding an alarm". See, for example, column 4, lines 16-22.

Referring to claim 8, Hile discloses:

"A computer readable medium, wherein the state table is stored upon the computer readable medium." See, for example, column 2, lines 4-7 and lines 36-42, column 3, lines 24-26 and column 4, lines 13-16.

Referring to claim 9, Hile discloses:

"The state machine comprises software code stored upon the computer readable medium, the software code further operable to be executed by a computer processor". See, for example, column 2, lines 36-42, column 4, lines 48-50 and column 5, lines 22-30.

Referring to claim 10, Hile discloses:

"The state machine is further operable to initialize the current state to an initial state". See, for example, column 4, lines 64-66.

Referring to claim 13, this claim is rejected as applied to the like elements of claims 1, 7, 14 and 20 above and further the following.

Hile discloses:

"A computer readable medium." See, for example, column 2, lines 4-7 and column 3, lines 24-26.

"A network interface for receiving an input stream comprising a plurality of characters." See, for example, column 1, lines 19-32 and Fig. 1 where the modem 28 is an example of a network interface.

"A processor communicatively coupled to the computer readable medium and the network interface". See, for example, column 2, lines 25-27 and lines 36-40, column 3, lines 17-24 and column 7, lines 39-44.

"A state table stored upon the computer readable medium, the state table indexed such that inputs comprising a current state and a current character yield an output of a new state, the new state related to an attack on a computer network". See, for example, column 4, lines 13-16 and column 4, line 59-column 5, line 21 where the machine state at start is zero and every next state and every incoming character are corresponding to the recited current state and current character, respectively, which are applied (inputted) to the state table to determine the next state of the machine. At the end, if checking of all characters of a string results in a predetermined machine state a virus match (intrusion detection) has occurred (indication of an attack).

"A state machine comprising instructions stored upon the computer readable medium and executable by the processor". See, for example, column 4, line 56-column 5, line 20.

"The state machine communicatively coupled to the state table". See, for example, column 2, line 36-42.

"The state machine operable to: maintain the current state". See, for example, Figure 3, where after each comparison step the resulting new state is maintained to be used as a current step for the next comparison step.

"Select a first character of the input stream as the current character and compare the current character and the current state to the state table to generate a new state". See, for example, column 4, line 66-column 5, line 20.

Referring to claim 21, Hile discloses:

"Setting the current state equal to the new state; selecting a next character as the current character, the next character appearing subsequent to the first character in the input stream; repeating the comparing step; and wherein the first character and the next character are each selected and compared only once." See, for example, column 4, line 59-column 5, line 21.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to

a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 6 and 19 are rejected under 35 USC 103(a) as being unpatentable over Hile et al. (5,319,776) (hereinafter Hile) in view of Ainsbury et al (6,078,924) (hereinafter Ainsbury).

Referring to claims 6 and 19, Hile does not expressly discloses:

"Generating the state table from a REGEX command". Ainsbury teaches that the REGEX (Regular Expression) are used to form tables. The Regular Expressions are commonly used in the art for parsing tables. See, for example, column 49, lines 57-67 and column 50, line 57-column 51, line 67.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the use of REGEX to generate state tables as taught in Ainsbury with the system of Hile, because it would provide state tables to be parsed by REGEX command to identify a pattern of character string.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No. 5,452,442 to Kephart

US Patent No. 6,205,551 B1 to Grosse

US Patent No. 5,586,266 to Hershey et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. N.

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN
April 14, 2004

Gilberto Barron

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100